Nevada Secretary of State
Voting System Testing and Security
Updated: August 2016

Voting system security is a complex process made up of several checks and balances. For example, the components of a voting system are not considered part of an official system until each component is thoroughly examined and continues to meet routine accuracy checks. The following describes the main testing and security procedures and how they interrelate. The attached diagram illustrates the related timing and flow of this process.

Pursuant to State Law voting system testing must be conducted by an Accuracy Certification Board and may be observed by the public. NRS 293B.140 and NRS 293B.145

Acceptance Testing
Before any component is considered part of the official voting system, it undergoes acceptance testing. This testing examines a system and its components to validate performance of delivered units and to and that the system is, in fact, the certified system purchased. Equipment that is suspected to be malfunctioning, have a broken chain of custody, or maliciously accessed, must be thoroughly investigated and pass acceptance tested before being brought back into the chain of custody.

Chain of Custody (NAC 293B.110)
Upon completion of acceptance testing, components are brought into a "trusted" environment that is maintained by a limiting access to authorized individuals, tamper evident security seals, and access audit logs. Each time a unit is accessed the tamper evident security seals are examined and checked against the access log. At any point that the chain of custody is broken, the cause must be investigated and appropriate testing must take place before equipment can be placed back into the chain of custody.

Certify Software, Firmware and Operating Systems (NAC 293B.110)
Before each election cycle, the software and firmware installed on each component of the voting system must be certified to match that versions approved for use and on file with the National Software Reference Library. This test is conducted by verifying the "hash" value of the software and firmware on each component and comparing it against the value on file with the National Software Reference Library. The hash value is an algorithm that maps the digital fingerprint of the code.

Logic and Accuracy Testing (NRS 293B.150, NRS 293B.155, NAC 293B.090)
Conducted before and after each election, this testing ensures that each component will accurately record, tally, and audit vote totals. This testing ensured that the contests are correctly reflected on equipment, all candidates and questions on a ballot can be voted on, and that results are accurately tabulated and reported. Local election officials use county-made test ballots with predetermined vote totals to test each component of the system, including but not limited to mechanical recording devices, tabulators, and Voter Verified Paper Audit Trails. Any error detected during these tests must be immediately reported to the Secretary of State.

(Continued on Page 2)

Security Audits and Ballot Reconciliation

Before, during and after voting, all components used during the election are routinely examined for unauthorized access. This includes examining tamper evident security seals that protect equipment access points as well as areas limited to authorized personnel, such as ballot and equipment storage areas. Equipment is also randomly selected and audited for accuracy. Auditing and reconciling equipment and ballots is completed by comparing the number of voters that have appeared and been checked in to vote match the number of ballots cast. These reconciliations take no less than daily and occur randomly while the polls are open.

Tabulation Certification (NRS 293B.165)

Tabulation equipment must be tested immediately before the start of the official count of the ballots and again within 24 hours after the official count takes place. This test is conducted by processing a preaudited group of logic and accuracy test ballots. If any errors are detected during these tests, the cause must be determined before the unit can be approved to tabulate ballots. The results of these tests are available for public inspection during the period a candidate may contest the election.

Postelection Audits (NAC 293B.120)

After each election, each county clerk shall audit the mechanical recording devices. The devices being audited are selected at random to verify that the hash value of the software and firmware installed matches that on file with the National Software Reference Library. Although law specifies a minimum number of units to be audited, Nevada's local election officials usually audit more units than required. In a county whose population is 100,000 or more, at least 2 percent but not less than 20 units must be audited. In a county whose populations less than 100,000, 3 percent but not less than four units must be audited.

Maintenance and Storage

Upon completion of the election cycle, each unit is evaluated for servicing before being placed in storage. Units requiring servicing are repaired and acceptance tested before being placed back into the chain of custody. All components of a voting system are securely stored with access audited and limited to authorized personnel. While in storage, system components are routinely monitored and maintained according to the applicable maintenance schedule. Before a voting system can be used in another election, it starts the process again, beginning with verifying the chain of custody while in storage and certifying the software, firmware and operating systems.